

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



دانشگاه تربیت مدرس

دانشکده مهندسی برق و کامپیوتر، گروه کامپیوتر

پایان نامه کارشناسی ارشد مهندسی کامپیوتر - نرم افزار

تشخیص رفتار غیرعادی در شبکه‌های اقتضایی مبتنی بر پروتکل مسیریابی OLSR

حجت گهرگزی

استاد راهنما:

دکتر سعید جلیلی

استاد مشاور:

دکتر مهدی آبادی

آبان ۱۳۹۱

آیین نامه حق مالکیت مادی و معنوی در مورد نتایج پژوهش‌های علمی دانشگاه تربیت مدرس

مقدمه: با عنایت به سیاست‌های پژوهشی و فناوری دانشگاه در راستای تحقق عدالت و کرامت انسانها که لازمه شکوفایی علمی و فنی است و رعایت حقوق مادی و معنوی دانشگاه و پژوهشگران، لازم است اعضای هیأت علمی، دانشجویان، دانش‌آموختگان و دیگر همکاران طرح، در مورد نتایج پژوهش‌های علمی که تحت عناوین پایان‌نامه، رساله و طرح‌های تحقیقاتی با هماهنگی دانشگاه انجام شده است، موارد زیر را رعایت نمایند:

ماده ۱- حق نشر و تکثیر پایان‌نامه/ رساله و درآمدهای حاصل از آنها متعلق به دانشگاه می باشد ولی حقوق معنوی پدید آورندگان محفوظ خواهد بود.

ماده ۲- انتشار مقاله یا مقالات مستخرج از پایان‌نامه/ رساله به صورت چاپ در نشریات علمی و یا ارائه در مجامع علمی باید به نام دانشگاه بوده و با تایید استاد راهنمای اصلی، یکی از اساتید راهنما، مشاور و یا دانشجو مسئول مکاتبات مقاله باشد. ولی مسئولیت علمی مقاله مستخرج از پایان‌نامه و رساله به عهده اساتید راهنما و دانشجو می باشد. تبصره: در مقالاتی که پس از دانش‌آموختگی بصورت ترکیبی از اطلاعات جدید و نتایج حاصل از پایان‌نامه/ رساله نیز منتشر می‌شود نیز باید نام دانشگاه درج شود.

ماده ۳- انتشار کتاب، نرم افزار و یا آثار ویژه (اثری هنری مانند فیلم، عکس، نقاشی و نمایشنامه) حاصل از نتایج پایان‌نامه/ رساله و تمامی طرح‌های تحقیقاتی کلیه واحدهای دانشگاه اعم از دانشکده‌ها، مراکز تحقیقاتی، پژوهشکده‌ها، پارک علم و فناوری و دیگر واحدها باید با مجوز کتبی صادره از معاونت پژوهشی دانشگاه و براساس آیین نامه‌های مصوب انجام شود. ماده ۴- ثبت اختراع و تدوین دانش فنی و یا ارائه یافته‌ها در جشنواره‌های ملی، منطقه‌ای و بین‌المللی که حاصل نتایج مستخرج از پایان‌نامه/ رساله و تمامی طرح‌های تحقیقاتی دانشگاه باید با هماهنگی استاد راهنما یا مجری طرح از طریق معاونت پژوهشی دانشگاه انجام گیرد.

ماده ۵- این آیین‌نامه در ۵ ماده و یک تبصره در تاریخ ۸۷/۴/۱ شورای پژوهشی و در تاریخ ۸۷/۴/۲۳ در هیأت رئیسه دانشگاه به تایید رسید و در جلسه مورخ ۸۷/۷/۱۵ شورای دانشگاه به تصویب رسیده و از تاریخ تصویب در شورای دانشگاه لازم‌الاجرا است.

«اینجانب حجت گهرگزی دانشجوی رشته مهندسی کامپیوتر- نرم افزار ورودی سال تحصیلی ۹۰-۱۳۸۹ مقطع کارشناسی ارشد دانشکده مهندسی برق و کامپیوتر متعهد می شوم کلیه نکات مندرج در آیین نامه حق مالکیت مادی و معنوی در مورد نتایج پژوهش‌های علمی دانشگاه تربیت مدرس را در انتشار یافته‌های علمی مستخرج از پایان‌نامه / رساله تحصیلی خود رعایت نمایم. در صورت تخلف از مفاد آیین نامه فوق‌الاشعار به دانشگاه وکالت و نمایندگی می‌دهم که از طرف اینجانب نسبت به لغو امتیاز اختراع بنام بنده و یا هر گونه امتیاز دیگر و تغییر آن به نام دانشگاه اقدام نماید. ضمناً نسبت به جبران فوری ضرر و زیان حاصله بر اساس برآورد دانشگاه اقدام خواهم نمود و بدینوسیله حق هر گونه اعتراض را از خود سلب نمودم»

امضا: حجت گهرگزی

تاریخ: ۹۱/۱۰/۲۴

آیین نامه چاپ پایان نامه (رساله) های دانشجویان دانشگاه تربیت مدرس

نظر به اینکه چاپ و انتشار پایان نامه (رساله) های تحصیلی دانشجویان دانشگاه تربیت مدرس، مبین بخشی از فعالیتهای علمی - پژوهشی دانشگاه است بنابراین به منظور آگاهی و رعایت حقوق دانشگاه، دانش آموختگان این دانشگاه نسبت به رعایت موارد ذیل متعهد می شوند:

ماده ۱: در صورت اقدام به چاپ پایان نامه (رساله) ی خود، مراتب را قبلاً به طور کتبی به «دفتر نشر آثار علمی» دانشگاه اطلاع دهد.

ماده ۲: در صفحه سوم کتاب (پس از برگ شناسنامه) عبارت ذیل را چاپ کند:

«کتاب حاضر، حاصل پایان نامه کارشناسی ارشد / رساله دکتری نگارنده در رشته مهندسی کامپیوتر - نرم افزار است که در سال ۱۳۹۱ در دانشکده مهندسی برق و کامپیوتر دانشگاه تربیت مدرس به راهنمایی جناب آقای دکتر سعید جلیلی، شاوره جناب آقای دکتر مهدی آبادی از آن دفاع شده است.»

ماده ۳: به منظور جبران بخشی از هزینه های انتشارات دانشگاه، تعداد یک درصد شمارگان کتاب (در هر نوبت چاپ) را به «دفتر نشر آثار علمی» دانشگاه اهدا کند. دانشگاه می تواند مازاد نیاز خود را به نفع مرکز نشر در معرض فروش قرار دهد.

ماده ۴: در صورت عدم رعایت ماده ۳، ۵۰٪ بهای شمارگان چاپ شده را به عنوان خسارت به دانشگاه تربیت مدرس، تأدیه کند.

ماده ۵: دانشجو تعهد و قبول می کند در صورت خودداری از پرداخت بهای خسارت، دانشگاه می تواند خسارت مذکور را از طریق مراجع قضایی مطالبه و وصول کند؛ به علاوه به دانشگاه حق می دهد به منظور استیفای حقوق خود، از طریق دادگاه، معادل وجه مذکور در ماده ۴ را از محل توقیف کتابهای عرضه شده نگارنده برای فروش، تامین نماید.

ماده ۶: اینجانب **حجت گهرگزی** دانشجوی رشته **مهندسی کامپیوتر - نرم افزار مقطع کارشناسی ارشد**

تعهد فوق و ضمانت اجرایی آن را قبول کرده، به آن ملتزم می شوم.

نام و نام خانوادگی: **حجت گهرگزی**

تاریخ و امضا: ۹۱/۱۰/۲۴



تاییدیه اعضای هیات داوران حاضر در جلسه دفاع از پایان نامه کارشناسی ارشد

آقای حجت گهرگزی پایان نامه ۶ واحدی خود را با عنوان تشخیص رفتار غیر عادی در شبکه های بیسیم اقتضایی مبتنی بر پروتکل مسیر یابی OLSR در تاریخ ۱۳۹۱/۸/۲۰ ارائه کردند.

اعضای هیات داوران نسخه نهایی این پایان نامه را از نظر فرم و محتوا تایید کرده، پذیرش آنرا برای اخذ درجه کارشناسی ارشد مهندسی کامپیوتر-ترنرم افزار پیشنهاد می کنند.

عضو هیات داوران	نام و نام خانوادگی	رتبه علمی	امضا
استاد راهنما	دکتر سعید جلیلی	دانشیار	
استاد مشاور	دکتر مهدی آبادی	استادیار	
استاد ناظر	دکتر محمد صنیعی آباده	استادیار	
استاد ناظر	دکتر سیاوش خرسندی	استادیار	
مدیر گروه (یا نماینده گروه تخصصی)	دکتر محمد صنیعی آباده	استادیار	

تقدیم بہ

پدر عزیز

و

مادر مہربانم

تشکر و قدردانی

الْحَمْدُ لِلَّهِ الَّذِي هَدَانَا لِهَذَا وَمَا كُنَّا لِنَهْتَدِيَ لَوْلَا أَنْ هَدَانَا اللَّهُ

سپاس خدای را که با یاری خویش بر من منت نهاد تا گامی دیگر در راه پیشرفت و اعتلای خود بردارم. امید آن که با بهره‌گیری مفید از آموخته‌ها و اندوخته‌های این دوره بتوانم شکرگزار بخش کوچکی از بیکران الطافش باشم.

با تشکر و سپاسگزاری از زحمات بی‌وقفه استاد گرامی جناب آقای دکتر جلیلی که همواره در طول این دوره با توصیه‌های خود، مسیر را بر من هموار نموده و مرا به مقصد مطلوب رهنمون شدند، و با تشکر از آقای دکتر آبادی که از مشاوره‌های ایشان بهره‌مند گردیدم.

همچنین از آقای رحمانی‌منش نیز به دلیل راهنمایی‌های سودمند ایشان در انجام این پژوهش قدردانی می‌نمایم.

بخشی از این پژوهش با حمایت مالی مرکز تحقیقات مخابرات ایران تحت قرارداد شماره ۱۹۲۳۰/۵۰۰ به انجام رسیده است.

حجت گهرگزی

آبان ماه ۱۳۹۱

چکیده

پروتکل OLSR به عنوان یکی از چهار پروتکل مسیریابی استاندارد برای شبکه های اقتضایی سیار، در برابر سوءرفتارهای انجام شده از جانب گره های مجاز شبکه آسیب پذیر است. سیستم های تشخیص نفوذ برای شناسایی این سوءرفتارها ارائه می شوند. سیستم تشخیص ناهنجاری نوعی از این سیستم هاست که سعی می کند رفتار غیر عادی را با یادگیری الگوی رفتار عادی شبکه شناسایی کند. یک مسئله مهم در مورد این سیستم ها مجموعه خصیصه هایی است که برای جمع آوری داده های مورد نیاز استفاده می نمایند. از آنجا که حمله های مختلف بر بخش های مختلف رفتار شبکه اثر می گذارند یک سیستم تشخیص ناهنجاری که از تعداد خصیصه های کم و نامناسب استفاده می کند قادر به تشخیص همه ناهنجاری ها نیست و از طرفی تعداد خصیصه های زیاد نیز ممکن است باعث کاهش دقت شود. به منظور ایجاد سیستم های تشخیص نفوذ در شبکه های اقتضایی که برای مسیریابی پروتکل OLSR را به کار می برند از دو رویکرد کلی استفاده می شود: تغییر و توسعه پروتکل، و روش های یادگیری ماشین. در این پژوهش ما مجموعه ای از خصیصه های پروتکل OLSR را برای پوشش تمام جنبه های رفتاری آن معرفی، و با استفاده از رویکرد یادگیری ماشین یک سیستم تشخیص ناهنجاری بر اساس جمع آوری مفهومی داده ها (CDC-ADS) ارائه می کنیم. این سیستم خصیصه ها را بر اساس منبع داده ها در چهار گروه در نظر گرفته و سپس یک الگو برای داده های عادی در هر گروه یادگیری می کند. برای تعیین عادی یا غیرعادی بودن یک رفتار، نظرات الگوهای یادگیری شده در رابطه با آن رفتار (شاخص های ناهنجاری) اخذ و تجمیع می گردند. ما برای تجمیع شاخص های ناهنجاری یک شیوه مبتنی بر انتخاب و میانگین گیری را معرفی می کنیم که بر طبق آن سه عدد از شاخص ها به عنوان خوش بین، بدبین، و علاقه مندی نمونه (شاخصی که نمونه مورد ارزیابی تمایل دارد با آن سنجیده شود) گزینش و از آن ها میانگین گیری می شود. آزمایشات نشان می دهد که جمع آوری داده ها در چهار گروه و ترکیب نظرات با شیوه مبتنی بر انتخاب و میانگین گیری، در مورد حمله های گوناگون نرخ تشخیص را افزایش و نرخ هشدار نادرست را کاهش می دهد. همچنین ارزیابی ها با شرایط گوناگون شبکه ای (سرعت ها و بازه های زمانی مختلف) بیانگر قدرت و جایگاه CDC-ADS می باشد.

کلید واژه: شبکه اقتضایی سیار، پروتکل OLSR، تشخیص ناهنجاری، دسته بندی تک کلاسی،

گروه متدها.

فهرست مطالب

صفحه	عنوان
	فهرست جدول‌ها
	فهرست شکل‌ها
	فهرست اختصارات
۱	فصل اول: کلیات.....
۱-۱-۱	پیشگفتار.....
۱-۲-۱	مسیریابی در شبکه های اقتضایی.....
۱-۳-۱	موضوع پژوهش.....
۱-۴-۱	نتایج حاصل از پژوهش.....
۱-۵-۱	مروری بر فصول پایان نامه.....
۹	فصل دوم: مفاهیم پایه و مبانی شبکه های اقتضایی مبتنی بر OLSR.....
۱-۱-۲	مقدمه.....
۱-۲-۲	پروتکل OLSR.....
۱-۲-۲-۱	ویژگی‌های پروتکل.....
۱-۲-۲-۲	قالب پیام‌ها.....
۱-۲-۲-۲-۱	قالب پیام HELLO.....
۱-۲-۲-۲-۲	قالب پیام TC.....
۱-۲-۲-۳	مخازن اطلاعات.....
۱-۲-۲-۴	رفتار پروتکل.....
۱-۲-۲-۴-۱	مسیریابی.....
۱-۲-۲-۴-۲	ارسال داده و مقابله با شکست مسیر.....
۱-۲-۲-۵	توسعه های پروتکل.....
۱-۲-۳	آسیب پذیری‌ها و ضعف های امنیتی پروتکل OLSR.....
۱-۳-۲	سوءرفتار در تولید پیام های کنترلی.....
۱-۳-۲	سوءرفتار در بازپخش پیام های کنترلی.....
۱-۴-۲	دسته بندی تک کلاسی.....
۱-۴-۲	روش های مبتنی بر چگالی.....

- ۲۷..... ۲-۴-۲ - روش های مبتنی بر مرز.....
- ۲۸..... ۳-۴-۲ - روش های مبتنی بر باز سازی.....
- ۲۹..... ۵-۲ - جمع بندی.....

فصل سوم: تاریخچه پژوهش در تشخیص نفوذ برای پروتکل OLSR..... ۳۱

- ۳۲..... ۱-۳ - مقدمه.....
- ۳۲..... ۲-۳ - رویکرد یادگیری ماشین.....
- ۳۲..... ۱-۲-۳ - سیستم توزیع شده سه سطحی.....
- ۳۳..... ۲-۲-۳ - سیستم CARRAD.....
- ۳۴..... ۳-۲-۳ - سیستم تشخیص رفتار فرو برنده.....
- ۳۴..... ۳-۳ - رویکرد توسعه پروتکل.....
- ۳۵..... ۱-۳-۳ - سیستم محاکمه‌ی توزیع شده.....
- ۳۶..... ۲-۳-۳ - کشف و جداسازی گره‌های بدخواه.....
- ۳۷..... ۳-۳-۳ - کاهش حملات ترافیک TC.....
- ۳۷..... ۴-۳-۳ - تشخیص حمله تبانی.....
- ۳۸..... ۵-۳-۳ - تشخیص حمله جداسازی گره.....
- ۳۸..... ۴-۳ - سایر رویکردها.....
- ۳۸..... ۱-۴-۳ - استدلال اعتباری خودکار.....
- ۳۹..... ۲-۴-۳ - تشخیص نفوذ بر اساس خصوصیت.....
- ۴۰..... ۳-۴-۳ - تشخیص با بررسی معنایی.....
- ۴۰..... ۴-۴-۳ - تشخیص بر مبنای ماشین حالت متناهی.....
- ۴۰..... ۵-۳ - تحلیل پژوهش های انجام شده.....
- ۴۲..... ۶-۳ - جمع بندی.....

فصل چهارم: مدل پیشنهادی..... ۴۳

- ۴۴..... ۱-۴ - مقدمه.....
- ۴۴..... ۲-۴ - خصیصه های رفتاری OLSR.....
- ۵۱..... ۳-۴ - سیستم تشخیص ناهنجاری.....
- ۵۲..... ۱-۳-۴ - جمع آوری مفهومی داده ها.....
- ۵۴..... ۲-۳-۴ - تجمیع نظرات.....
- ۵۴..... ۱-۲-۳-۴ - تجمیع بر اساس وزن دهی.....
- ۵۵..... ۲-۲-۳-۴ - تجمیع بر اساس انتخاب و میانگین گیری.....

۵۶..... روش مقیاس گذاری..... ۳-۳-۴

۵۷..... جمع بندی..... ۴-۴

فصل پنجم: ارزیابی سیستم تشخیص نفوذ بر اساس جمع آوری مفهومی داده (CDC-ADS) ۵۸.

۵۹..... مقدمه..... ۱-۵

۵۹..... مدل ارزیابی..... ۲-۵

۶۰..... شبیه سازی..... ۳-۵

۶۱..... ویژگی های شبیه سازی..... ۱-۳-۵

۶۲..... پیاده سازی حملات..... ۲-۳-۵

۶۳..... نتایج ارزیابی CDC-ADS..... ۴-۵

۶۳..... انتخاب روش یادگیری..... ۱-۴-۵

۶۴..... تاثیر خصیصه های تعریف شده و ارزیابی آن ها..... ۲-۴-۵

۶۹..... بررسی CDC-ADS و پیمانانه تجمیع نظرات..... ۳-۴-۵

۷۲..... بررسی سرعت های مختلف حرکت گره ها در شبکه..... ۴-۴-۵

۷۷..... مقایسه CDC-ADS با CFA/C4.5 [۹]..... ۵-۴-۵

۸۰..... مقایسه CDC-ADS با سایر روش ها..... ۶-۴-۵

۸۲..... جمع بندی..... ۵-۵

فصل ششم: نتیجه گیری و پیشنهادات..... ۸۳

۸۴..... نتیجه گیری..... ۱-۶

۸۵..... پیشنهادات..... ۲-۶

۸۷..... فهرست مراجع.....

پیوست: فیلد های بسته ها، پیام ها و جداول در OLSR

واژه نامه ی فارسی به انگلیسی

واژه نامه ی انگلیسی به فارسی

فهرست جدول‌ها

عنوان	صفحه
جدول ۱-۲: خطای نوع اول و خطای نوع دوم.....	۲۶
جدول ۱-۳: مقایسه سیستم‌های مبتنی بر رویکرد یادگیری ماشین.....	۳۵
جدول ۲-۳: مقایسه سیستم‌های تشخیص نفوذ که با توسعه پروتکل عمل می‌کنند.....	۳۹
جدول ۳-۳: مقایسه سایر رویکردهای تشخیص ناهنجاری.....	۴۰
جدول ۱-۴: فهرست خصیصه‌های خام مستخرج از پروتکل OLSR.....	۴۵
جدول ۲-۴: خصیصه‌های بسته‌ها.....	۴۶
جدول ۳-۴: خصیصه‌های جداول.....	۴۷
جدول ۴-۴: خصیصه‌های پیام HELLO.....	۴۸
جدول ۵-۴: خصیصه‌های پیام TC.....	۴۹
جدول ۶-۴: گروه‌های چهارگانه خصیصه‌ها، تعداد و توصیف آن‌ها.....	۵۳
جدول ۱-۵: پارامترهای شبیه‌سازی.....	۶۱
جدول ۲-۵: مقادیر AUC، مقایسه روش‌های SOM، MoG و K-means.....	۶۵
جدول ۳-۵: مقایسه مقادیر AUC با توجه به کاهش ابعاد با مقادیر مختلف POV.....	۶۹
جدول ۴-۵: مقایسه مقادیر AUC برای روش‌های تجمیع متفاوت، و درصد بهبود AUC به ازای همه حملات.....	۷۲
جدول ۵-۵: مقایسه مقادیر AUC تک مدل و CDC-ADS با روش‌های تجمیع متفاوت برای سرعت‌های مختلف.....	۷۷
جدول ۶-۵: مقایسه مقادیر AUC برای CDC-ADS و CFA/C4.5.....	۸۱
جدول ۷-۵: مقایسه کلی CDC-ADS و سایر سیستم‌های ارائه شده.....	۸۲

فهرست شکل ها

عنوان	صفحه
شکل ۱-۱: پروتکل های مسیریابی شبکه های اقتضایی.....	۴
شکل ۱-۲: بازپخش.....	۱۱
شکل ۲-۲: قالب بسته ها در OLSR.....	۱۲
شکل ۳-۲: قالب پیام های HELLO.....	۱۴
شکل ۴-۲: فیلد Link Code در پیام HELLO.....	۱۴
شکل ۵-۲: قالب پیام های TC.....	۱۵
شکل ۶-۲: الگوریتم انتخاب MPR.....	۱۷
شکل ۷-۲: مسیریابی در OLSR.....	۱۷
شکل ۸-۲: انواع حملات روی پیام های کنترلی پروتکل OLSR.....	۲۲
شکل ۹-۲: دسته بند تک کلاسی.....	۲۵
شکل ۱۰-۲: ترکیب چند توزیع نرمال (MoG).....	۲۶
شکل ۱۱-۲: توصف داده بردار پشتیبان.....	۲۸
شکل ۱۲-۲: روش SOM.....	۲۹
شکل ۱-۴: بررسی تغییرات خصیصه های مختلف با مقایسه میانگین مقادیر آن ها.....	۵۰
شکل ۲-۴: معماری مدل اولیه سیستم تشخیص ناهنجاری با آموزش برون خط.....	۵۱
شکل ۳-۴: معماری تفصیلی ADS معرفی شده با جمع آوری مفهومی داده.....	۵۲
شکل ۴-۴: پیمانه تجمیع نظرات بر اساس انتخاب و میانگین گیری.....	۵۶
شکل ۱-۵: منحنی ROC.....	۶۰
شکل ۲-۵: مقایسه روش های SOM، MOG و k-means برای انتخاب روش یادگیری.....	۶۴
شکل ۳-۵: مقایسه خصیصه های تعریف شده در بخش ۴-۱ با خصیصه های معرفی شده در [۹].....	۶۶
شکل ۴-۵: اعمال PCA با POV مختلف (۱، ۰/۹۵، ۰/۹ و ۰/۸۵). سرعت 5 m/s و بازه زمانی 30 s و اجرای SOM.....	۶۷
شکل ۵-۵: اعمال PCA با POV مختلف (۱، ۰/۹۵، ۰/۹ و ۰/۸۵). سرعت 5 m/s و بازه زمانی 60 s و اجرای SOM.....	۶۸
شکل ۶-۵: ارزیابی CDC-ADS با توجه به روش های مختلف ترکیب و حالت "تک مدل". سرعت 5 m/s و بازه زمانی 30 s.....	۷۰

- شکل ۵-۷: ارزیابی CDC-ADS با توجه به روش های مختلف ترکیب و حالت "تک مدل". سرعت 5 m/s و بازه زمانی 60 s ۷۱
- شکل ۵-۸: مقایسه CDC-ADS با توجه به دو روش ترکیب، با حالت "تک مدل". سرعت 10 m/s و بازه زمانی 30 s ۷۳
- شکل ۵-۹: مقایسه CDC-ADS با توجه به دو روش ترکیب، با حالت "تک مدل". سرعت 10 m/s و بازه زمانی 60 s ۷۴
- شکل ۵-۱۰: مقایسه CDC-ADS با توجه به دو روش ترکیب، با حالت "تک مدل". سرعت 15 m/s و بازه زمانی 30 s ۷۵
- شکل ۵-۱۱: مقایسه CDC-ADS با توجه به دو روش ترکیب، با حالت "تک مدل". سرعت 15 m/s و بازه زمانی 60 s ۷۶
- شکل ۵-۱۲: مقایسه CDC-ADS و CFAC4.5. سرعت 5 m/s و بازه زمانی 30 s ۷۸
- شکل ۵-۱۳: مقایسه CDC-ADS و CFAC4.5. سرعت 5 m/s و بازه زمانی 60 s ۷۹
- شکل ۵-۱۴: مقایسه نرخ تشخیص در CDC-ADS و CFA/C4.5 برای FAR=0 ۸۰

فهرست اختصارات

علامت اختصاری	شرح
ADS	Anomaly Detection System
CARRADS	Cross layer based Adaptive Real-time Routing Attack Detection System
CDC-ADS	Conceptual Data Collection based Anomali Detection System
DoS	Denial of Service
IDS	Intrusion Detection System
MANET	Mobile Ad hoc Network
MDS	Misuse Detection System
MPR	Multi Point Relay
OCC	One-Class Classification
OLSR	Optimized Link State Routing
OPTI	Optimistic Index
PESI	Pessimistic Index
SFI	Sample Favorite Index
SOM	Self Organizing Map

فصل اول:

کلیات

۱-۱- پیشگفتار

شبکه های کامپیوتری از سال های آغازین پیدایش ریزکامپیوترها مورد توجه قرار گرفتند. با گسترش فناوری های مخابراتی، شبکه های بی سیم به وجود آمدند، در کنار شبکه های سیمی توسعه یافتند و همچنان در مجامع تحقیقاتی و حوزه کاربرد، جزء مباحث روز به شمار می روند.

شبکه های بی سیم از نظر شالوده و زیربنا به دو دسته باساختار^۱ و اقتضایی^۲ (بدون ساختار) تقسیم می شوند. شبکه های دارای ساختار توسط نقاط دسترسی به یک شبکه سیمی بزرگ متصل می گردند اما شبکه های اقتضایی، میزبان های بی سیمی هستند که به صورت خود سازمان یافته با یکدیگر ارتباط برقرار می کنند.

شبکه های اقتضایی سیار^۳، یک مجموعه از گره های سیار بی سیم را شامل می شود که می توانند به صورت پویا و مستقل از شبکه های دیگر خود را در یک همبندی اختیاری و موقت سازمان دهی کنند و به این وسیله به افراد و ابزار اجازه دهند تا به طور مداوم در محدوده ای که هیچ زیرساخت از پیش تعیین شده ای وجود ندارد با هم ارتباط داشته باشند [۱].

گسترش و پیشرفت ابزارهای ارتباطی سیار از جمله تلفن سلولی و کامپیوترهای قابل حمل، انقلابی در جامعه اطلاعاتی بوجود آورده است، ابزارهایی که هر روز قوی تر و ارزان تر می شوند. ما در حال گذر از نسل کامپیوترهای شخصی به نسل کامپیوترهای همه جا حاضر هستیم. طبیعت این کامپیوترها این الزام را به وجود می آورد که شبکه ها به صورت بی سیم باشند، بنابراین زمینه شبکه های بی سیم در حال رشد نمایی است [۲]. شبکه های اقتضایی علاوه بر مسائل شبکه های بی سیم معمولی، با چالش های منحصر به فردی نیز رو به رو هستند، از جمله می توان به موارد زیر اشاره کرد [۲]:

- زیرساخت ثابتی در این شبکه ها وجود ندارد.

¹ Infrastructure

² Ad hoc

³ Mobile Ad hoc Network (MANET)

- در این شبکه ها مسیریاب اختصاصی وجود ندارد.
- سرویس ها (بی مانند مدیریت شبکه) در این شبکه ها باید توزیع شده باشند.
- کانال مورد استفاده از سیگنال های دیگر محافظت نمی شود.
- این شبکه ها قابلیت اطمینان بسیار پایینتری دارند.
- همبندی این شبکه ها پویا است.
- قدرت گره ها در حال تغییر و انرژی آنها محدود است.

۱-۲- مسیریابی در شبکه های اقتضایی

طبیعت پویای شبکه های بی سیم اقتضایی باعث می شود همبندی شبکه مکررا و به صورت غیرقابل پیش بینی تغییر کند، که این باعث پیچیدگی مسیریابی در میان گره های شبکه می شود. جنبه دیگر این پیچیدگی لزوم مشارکت تمام گره های شبکه در فرآیند مسیریابی است. بر این اساس پروتکل های متفاوتی به منظور مسیریابی معرفی شده اند که هر کدام سعی می کنند به نحوی این مسئله را حل نمایند.

پروتکل های مسیریابی در شبکه های بی سیم اقتضایی به سه دسته: پیش گستر^۱، واکنشی^۲ و ترکیبی تقسیم می شوند (شکل ۱-۱). پروتکل های پیش گستر تلاش می کنند تا اطلاعات مسیریابی را به روز نگه دارند. برای این کار، بسته به طراحی، هر گره اطلاعات به روز خود را بین همسایگان خود و یا در کل شبکه پخش می کند. زمان توزیع این اطلاعات می تواند به صورت دوره ای و یا برحسب وقوع رخداد در نظر گرفته شود. به بیان دیگر با استفاده از این پروتکل ها، هر گره در هر زمان مسیر به سایر گره ها را می داند. از آنجا که این پروتکل ها اطلاعات خود را در جدول نگهداری می کنند، به پروتکل های بر مبنای جدول نیز معروف هستند. مهمترین پروتکل های پیش گستر عبارتند از: OLSR^۳ و TBRPF^۴ [۳].

پروتکل های واکنشی بر خلاف پروتکل های پیش گستر تنها زمانی بین دو گره مسیر ایجاد می کنند که بسته ای برای ارسال وجود داشته باشد. در این هنگام مبدأ از طریق فرایند کشف مسیر، مسیر مورد نظر را ایجاد می کند. این مسیر تا زمانی نگهداری می شود که دیگر بسته ای برای ارسال وجود نداشته

¹ Proactive

² Reactive

³ Optimized Link State Routing (RFC3626)

⁴ Topology dissemination Based on Reverse Path Forwarding (RFC 3684)

باشد، یا گره مقصد غیرقابل دسترس شود، و یا زمان استفاده از آن به پایان برسد. از مهمترین این پروتکل ها می توان ¹AODV و ²DSR را نام برد [۳].



شکل ۱-۱: پروتکل های مسیریابی شبکه های اقتضایی

دسته سوم، ترکیبی از پروتکل های پیش گستر و واکنشی را مورد استفاده قرار می دهند به این صورت که مسیرهای موجود در بخش هایی از شبکه را به طور دائم نگهداری کرده و برای سایر بخش ها (معمولا فواصل دور) در هنگام نیاز مسیر را ایجاد می کنند. پروتکل های ³ZRP و HOPNET نمونه هایی از این دسته می باشند [۳، ۴].

بعضی از خصوصیات که باید در طراحی پروتکل های مسیریابی مورد توجه قرار گیرد عبارتند از: منابع محدود، تعامل همبندی متغیر، مقیاس پذیری، پشتیبانی از ارتباطات یک طرفه، اطمینان، امنیت، و پشتیبانی از کیفیت سرویس [۲].

۱-۳- موضوع پژوهش

همچون هر سیستم کامپیوتری، یکی از مهم ترین مباحث شبکه های اقتضایی، مسئله امنیت است. با در نظر گرفتن ویژگی های منحصر به فرد این شبکه ها به ویژه در لایه شبکه، امنیت این لایه اهمیت بیشتری پیدا می کند.

ماهیت بی سیم بودن، تحرک داشتن، و فقدان ساختار اولیه و مسیریاب ثابت سبب شده است تا شبکه های اقتضایی ویژگی های منحصر به فردی داشته باشند که نمود واقعی آن ها در لایه شبکه و مسیریابی است. در این شبکه ها تمام گره ها باید علاوه بر انجام وظایف عادی خود، مانند مسیریاب عمل

¹ Ad hoc On demand Vector Distance (RFC 3561)

² Dynamic Source Routing (RFC 4728)

³ Zone Routing Protocol

کرده و در فرآیند مسیریابی شرکت نمایند. از طرفی نکته قابل توجه در مورد پروتکل های مسیریابی این است که آن ها همه گره های شبکه را سالم و درستکار فرض می کنند، لذا هیچ گونه تمهیدات امنیتی^۱ در آن ها در نظر گرفته نشده است. در نتیجه گره های بدخواه^۲ می توانند به راحتی باعث ایجاد اختلال در کار شبکه و یا حتی فروپاشی کامل آن شوند.

سوء رفتار^۳ در شبکه های اقتضایی از رفتارهای نادرست و ناخواسته گره ها و یا حملات، که می توانند از جانب گره (های) متخاصم خارجی و یا گره (های) بدخواه داخلی روی دهند، ناشی می شود. برای مقابله با سوء رفتارها به طور کلی دو رویکرد مورد توجه قرار گرفته است: (۱) افزودن بعضی مکانیزم های امنیتی مانند تصدیق اصالت^۴ به پروتکل مسیریابی و (۲) ایجاد سیستم های تشخیص نفوذ^۵. سیستم های تشخیص نفوذ از دید روش تشخیص، در دو دسته تشخیص ناهنجاری (رفتار غیرعادی)^۶ و تشخیص سوء استفاده^۷ گروه بندی می شوند [۵].

سیستم های مبتنی بر تشخیص ناهنجاری، سعی می کنند تا با استفاده از روش های یادگیری، الگوهای رفتار عادی شبکه را ایجاد نمایند، از آن پس هرگونه رفتار مغایر با الگوهای شناخته شده، سوء رفتار تشخیص داده می شود. مزیت این رویکرد کشف حملاتی است که تاکنون ناشناخته بوده اند، اما معمولاً نرخ هشدار نادرست^۸ آن زیاد است. در مقابل، سیستم های تشخیص سوء استفاده، الگوی هر بد رفتاری خاص را شناسایی و یادگیری کرده و مواردی را که با آن تطابق داشته باشد به عنوان بد رفتاری یا حمله اعلام می کنند. این سیستم ها به نسبت سیستم های تشخیص ناهنجاری، نرخ هشدار نادرست پایینتری دارند، اما امکان تشخیص حملات نو و ناشناخته وجود ندارد [۵].

پروتکل مسیریابی OLSR به عنوان یکی از چهار پروتکل استاندارد ارائه شده برای شبکه های اقتضایی و مهمترین پروتکل پیش گستر، در حال حاضر در مجامع تحقیقاتی و همچنین کاربرد مورد توجه قرار گرفته است. دلایل این توجه را باید در تغییر ماهیت شبکه های اقتضایی از شبکه هایی با کاربرد نظامی به شبکه های عمومی تر مانند شبکه های ارتباطی تیم های امداد و نجات و یا حتی شبکه های سرگرمی جستجو کرد که محیط های بزرگ و متراکم، و نیازهای جدیدی مانند کیفیت سرویس^۹ را مطالبه می کند.

¹ Security Measures

² Malicious

³ Misbehavior

⁴ Authentication

⁵ Intrusion Detection System (IDS)

⁶ Anomaly Detection System (ADS)

⁷ Misuse Detection System (MDS)

⁸ False Alarm Rate

⁹ Quality of Service (QoS)